International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

"EIGAMAL SIGNATURE SCHEME" - APPROACH TO ENSURING THE SECURITY OF CLOUD COMPUTING ENVIRONMENT

Manisha Malhotra

MCA-Department

Maharishi Markandeshwar University-Mullana-Ambala

Abstract

Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors.

1. Introduction of Main Security Issues:

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

At the heart of cloud infrastructure is this idea of multi-tenancy and decoupling between specific hardware resources and applications, In the jungle of multi-tenant data, we need to trust the cloud provider that your information will not be exposed. For their part, companies need to be vigilant, for instance about how passwords are assigned, protected and changed. Cloud service providers typically work with numbers of third parties, and customers are advised to gain information about those companies which could potentially access their data. So in the raw era the main issue of cloud computing is security.

Figure 1:Cloud Infrastructure

The main Security issues in cloud computing are as follows:

- Data security
- Network security
- Data locality

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

- Data integrity
- Data segregation
- Data access
- Authentication and authorization
- Data confidentiality
- Web application security
- Virtualization vulnerability
- Availability
- Backup

From the above said issuses, this paper explore the data security of cloud computing.

2. Data Security Problems in Cloud Computing:

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

Whether the IBM's Blue Cloud or the Microsoft's Windows Azure, the virtual machine technology is considered as a cloud computing platform of the fundamental component, the differences between Blue Cloud and Windows zure is that virtual machine running on Linux operating system or Microsoft Windows operating system. Virtual Machine technology bring obvious advantages, it allows the operation of the server which is no longer dependent on the physical device, but on the virtual servers. In virtual machine, a physical change or migration does not affect the services provided by the service provider. if user need more services, the provider can meet user's needs without having to concern the physical hardware. However, the virtual server from the logical server group brings a lot of security problems. The traditional data center security measures on the edge of the hardware platform, while cloud computing may be a server in a number of virtual servers, the virtual server may belong to different logical server group, virtual server, therefore there is the possibility of attacking each other ,which brings virtual servers a lot of security threats. Virtual machine extending the edge of clouds makes the disappearance of the network boundary, thereby affecting almost all aspects of security, the traditional physical isolation and hardware-based security infrastructure can not stop the clouds computer environment of mutual attacks between the virtual machine.

2.1 Consistency of Data

Cloud environment is a dynamic environment, where the user's data transmits from the data centre to the user's client. For the system, the user's data is changing all the time. Read and write data relating to the identity of the user authentication and permission issues. In avirtual machine, there may be different users' data which must be strict managed. The traditional model of access control is built in the edge of computers, so it is weak to control reading and writing among distributed computers. It is clear that traditional access control is obviously

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

not suitable for cloud computing environments. In the cloud computing environment, the traditional access control mechanism has serious shortcomings.

2.2 Principle of Data Security

All the data security technique is built on confidentiality, integrity and availability of these three basic principles. Confidentiality refers to the so-called hidden the actual data or information, especially in the military and other sensitive areas, the confidentiality of data on the more stringent requirements. For cloud computing, the data are stored in "data center", the security and confidentiality of user data is even more important. The so-called integrity of data in any state is not subject to the need to guarantee unauthorized deletion, modification or damage. The availability of data means that users can have the expectations of the use of data by the use of capacity. For the security of data the approach is to be used in this paper is Digital Signatures.

2.3 Approach used For Data Security-Digital Signature:

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries, including the United States, India, and members of the European Union, electronic signatures have legal significance. However, laws concerning electronic signatures do not always make clear whether they are digital cryptographic signatures in the sense used here, leaving the legal definition, and so their importance, somewhat confused.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

A digital signature scheme typically consists of three algorithms:

- A *key generation* algorithm that selects a *private key* uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding *public key*.
- A *signing* algorithm that, given a message and a private key, produces a signature.

Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key. A *signature verifying* algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity. This paper used “The ElGamal signature scheme”(is a digital signature scheme which is based on the difficulty of computing discrete logarithms). It was described by Taher ElGamal in 1984. A variant developed at NSA and known as the Digital Signature Algorithm is much more widely used. There are several other variants. The ElGamal signature scheme must not be confused with ElGamal encryption which was also invented by Taher ElGamal. The ElGamal signature scheme allows that a verifier can confirm the authenticity of a message *m* sent by the signer sent to him/her over an insecure channel.

Parameters to be used: These system parameters may be shared between users.

- Let *H* be a collision-resistant hash function.
- Let *p* be a large prime such that computing discrete logarithms modulo *p* is difficult.
- Let $g < p$ be a randomly chosen generator of the multiplicative group of integers modulo *p* Z_p^*.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

/*How to generate a key

- Choose randomly a secret key x with $1 < x < p - 1$.
- Compute $y = g^x \bmod p$.
- The public key is (p, g, y).
- The secret key is x.

These steps are performed once by the signer.

Signature generation : To sign a message m the signer performs the following steps.

- Choose a random k such that $0 < k < p - 1$ and $\gcd(k, p - 1) = 1$.
- Compute $r \equiv g^k \pmod{p}$.
- Compute $s \equiv (H(m) - xr)k^{-1} \pmod{p-1}$.
- If $s = 0$ start over again.

Then the pair (r,s) is the digital signature of m. The signer repeats these steps for every signature. Now this signature must be veirfy. A signature (r,s) of a message m is verified as follows.

- $0 < r < p$ and $0 < s < p - 1$.
- $g^{H(m)} \equiv y^r r^s \pmod{p}$.

The verifier accepts a signature if all conditions are satisfied and rejects it otherwise.

Security provide

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

A third party can forge signatures either by finding the signer's secret key *x* or by finding collisions in the hash function $H(m) \equiv H(M) \pmod{p-1}$. Both problems are believed to be difficult. The signer must be careful to choose a different *k* uniformly at random for each signature and to be certain that *k*, or even partial information about *k*, is not leaked. Otherwise, an attacker may be able to deduce the secret key *x* with reduced difficulty, perhaps enough to allow a practical attack.

3. Conclusion and Future Work:

So by using ElGamal Signature scheme , the data security can be controlled at some extent. Cloud Provider whose provide services to the vendors can be assure for this security. The main thing which is always have to be remembered for vendor i.e he/she have to be cared before choosing a k uniformity. If partial information is being leaked by signer then an attacker may be know the secret key x . in future implements more algorithm or revised of this to improve the security.

References:

[1] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing,” Proc. 14th European Symp. Research in Computer Security (ESORICS ’09), pp. 355-370, 2009.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 598-609, 2007.

[3] R.C. Merkle, “Protocols for Public Key Cryptosystems,” Proc. IEEE Symp. Security and Privacy, pp. 122-133, 1980. [18] S. Lin and D.J. Costello, Error Control Coding, second ed., Prentice- Hall, 2004.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

[4] M. Bellare and P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," Proc. First ACM Conf. Computer and Comm. Security (CCS '93), pp. 62-73, 1993.

[5] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22ndInt'l Conf. Theory and Applications of Cryptographic techniques (Eurocrypt '03), pp. 416-432, 2003.

[6] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Cryptology ePrint Archive, Report 2008/175, 2008 http://eprint.iacr.org/.

[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, "Provable Data Possession at Untrusted Stores," *Proc. Of CCS '07*, pp. 598–609, 2007.

[8] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession,"*Proc. Of SecureComm '08*, pp. 1–10, 2008.

[9] T. S. J. Schwarz and E. L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," *Proc.of ICDCS '06*, pp. 12–12, 2006.